DENCRYPT SECURE TALK
ENCRYPTED MOBILE COMMUNICATION

Industrial espionage is a growing problem and we see more frequent and more sophisticated attacks. Also mobile security becomes increasingly important to protect company assets and confidential information. Today, companies, governments and organisations cannot be sure that private and confidential conversations remain secret.

DENCRYPT SECURE TALK OFFERS

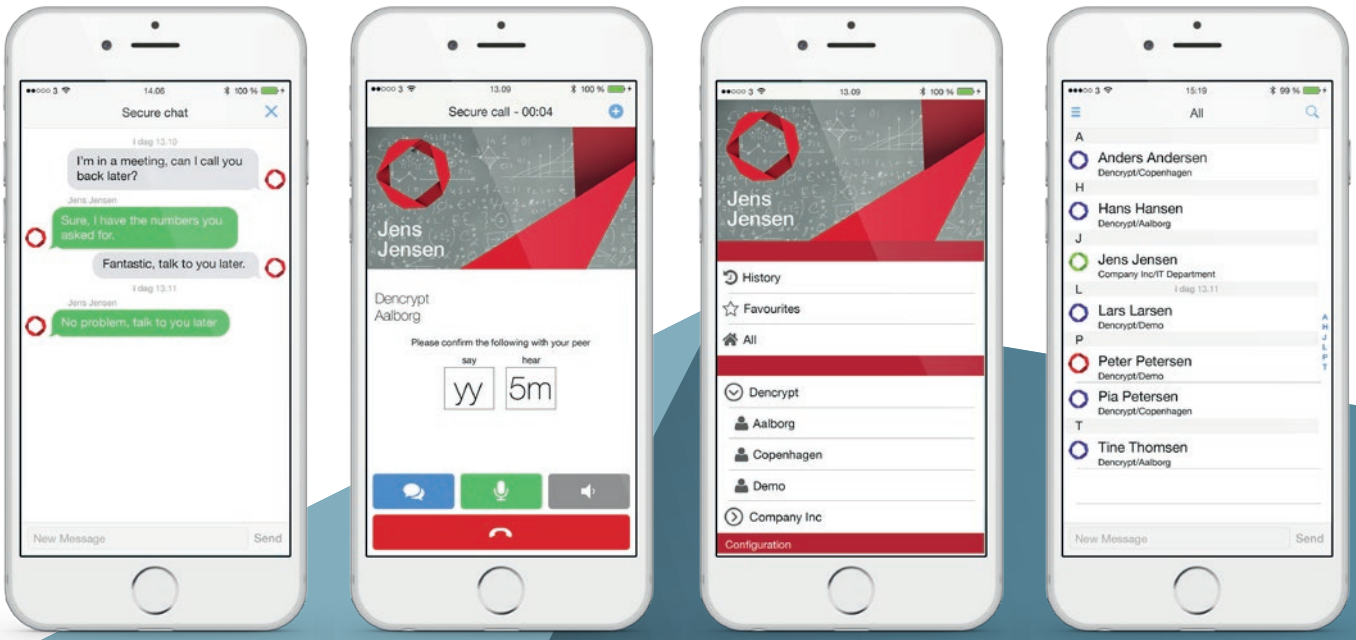
DYNAMIC ENCRYPTION

USER-FRIENDLY OPERATION

INTEGRATED TO YOUR SMARTPHONE

FEATURE SET

- Encrypted end-to-end voice calls over VoIP
- Encrypted live chat
- Encrypted group call
- Secured call setup via a dedicated SIP server
- High audio quality
- Secure individual phone book
  - Centrally managed
  - Pushed seamlessly to user devices
  - Supports individual groups settings
- Individual ring tones
- In call functionality: Mute, speaker
- Seemless over-the-air SW updates
- Connectivity on all cellular and wireless networks including:
  - GSM/EDGE, WCDMA/HSPA, LTE, WiFi
- Support all major mobile platforms
  - iOS and Android
  - Windows phone (on request)



Version 1.0

DENCRYPT

DENCRYPT SECURE TALK
TECHNICAL SPECIFICATIONS

Voice & data encryption
Secure end-to-end encrypted voice and chat using dynamic encryption, which ensures that each call session is encrypted using a randomly chosen algorithm and a randomly chosen key.

- Dynamic encryption of voice data implemented as multiple layers of encryption optimized for voice data over the SRTP protocol:
  - 2 x 128-bit whitening keys as an additional layer to a standard AES-256 encryption.
  - 128-bit key dynamic encryption for defining an addition AES-round with randomly chosen S-boxes.
  - Patent pending: PCT/EP2012/071314.
- 3072 bit Diffie-Hellman with 256 hash function for key exchange over the zRTP protocol.
- SAS: 4-letter readout has based key authentication.
- Encryption key and algorithm is established at call setup and destroyed as soon as call is terminated.
- Random number generation using Yarrow algorithm on iOS.

Server authentication
Secure server authentication and registration for call setup and user account management.

- SIP Secure + TLS1.2 using AES-256-GCM for data protection and ECDHE-RSA for key exchange using a 4096 bit certificate.

Connectivity
Voice-over-IP calls and chat over all cellular and wireless networks, including:

- GSM/EDGE, WCDMA/HSPA, LTE/LTE-A, Wireless LAN.

Audio
Adaptive audio quality based on current network conditions, Supported audio codecs:

- SPEEX, OPUS
- Polyphonic ringtones

Performance
- Same or better voice quality as non-encrypted voice-over-IP calls. Encryption does not introduce an audible delay nor a voice quality degradation.
- Fast call setup time and high reliability.
- Same battery power consumption as other VoIP-clients ensuring a similar talk time and standby time.

Supported platforms
- iOS 7.0 and later.
- Android 4.x (Jelly Bean) and later.

Contact:

Dencrypt A/S
Arnold Nielsens
Boulevard 72-74, 1. Sal
2650 Hvidovre
DENMARK

+45 7211 7911
info@dencrypt.dk
www.dencrypt.dk

Version 1.0